UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,214	04/18/2001	Peter T. Dinsmore	NAI1P089/00.175.01	6427

28875   7590   02/09/2009
Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER
LAFORGIA, CHRISTIAN A

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	09/836,214	DINSMORE ET AL.
	Examiner	Art Unit	
	Christian LaForgia	2439	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>23 January 2009</u>.

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>13-15,19-21,41-45 and 48-50</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>13-15, 19-21,41-45 and 48-50</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on <u>07 September 2001</u> is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
         application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1.   A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after a pre-appeal request. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 23 January 2009 has been entered.

2.   Claims 13-15, 19-21, 41-45 and 48-50 have been presented for examination.

3.   Claims 1-12, 16-18, 22-40, 46, and 47 have been cancelled as per Applicant's

amendment.

Response to Arguments

4.   Applicant's arguments filed 23 January 2009 have been fully considered but they are not

persuasive.

5.   It appears that the Applicant has failed to address the Examiner's rejection that the

claimed invention was publicly used more than one year prior to the filing of the patent

application, thereby creating a statutory bar. The Applicant is required to address this rejection

in response to this Office Action or face receiving a non-responsive amendment for failing to

address all the rejections set forth.

6.   The Applicant renews their arguments that Balenson does not specifically teach wherein

the determining uses a function having the following properties: (1) knowledge of said updated

first key does not give knowledge of said first key or said second key, (2) knowledge of said first

key does not give any knowledge of said updated first key, and (3) knowledge of said first key

and said updated first key does not give any knowledge of said second key on pages 6-8. The

Examiner has afforded the limitation very little patentable weight since wherein clauses in

method claims are not given weight when they simply express the intended result of a process

step positively recited. See *Texas Instruments Inc. v. U.S. International Trade Commission*, 988

F.2d 1165 (Fed. Cir. 1993). In this case the wherein clause merely expresses properties that

result from the determining step. In other words, the properties disclosed in the wherein clause

do not provide any information regarding the mechanics of how the determining step is executed.

See *Minton v. National Association of Securities Dealers, Inc.*, 67 USPQ2d 1614, 1620 (Fed.

Cir. 2003). See also MPEP § 2111.04. Since very little patentable weight is given to the

wherein clauses in both independent claims 13 and 43, the rejection is maintained, albeit clarified

below which provides for the present non-final rejection.

7.   Furthermore, in regards to the Applicant's arguments on pages 6 and 7 that Balenson

does not specifically teach wherein the determining uses a function having the following

properties: (1) knowledge of said updated first key does not give knowledge of said first key or

said second key, (2) knowledge of said first key does not give any knowledge of said updated

first key, and (3) knowledge of said first key and said updated first key does not give any

knowledge of said second key, the Applicant never states that the properties are not for the

collusion resistance and merely argues that the reference is not as specific as the claim language.

This amounts to a general allegation that the claims define a patentable invention without

specifically pointing out how the language of the claims patentably distinguishes them from the

references, especially since the applicant never says that the properties are not for collusion

resistance. Therefore, even if the "wherein" clause is afforded patentable weight, the reference

still provides a teaching of the claimed properties.

8.   The Applicant further argues that the prior art does not disclose the amended claim

limitations in independent claims 13 and 43. The Examiner disagrees. The limitation recites

wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way

function. The Examiner refers the Applicant to pages 10 and 11, figures 2 and 3, respectively,

which disclose $k_i = f(k'_x, k'_y)$ in a one-way function tree. Since DCCM discloses the newly

added limitation in at least Figures 2 and 3, the rejection is maintained.

9.   See further rejections set forth below.

Claim Rejections - 35 USC § 101

10.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

11.   Claims 13-15, 19-21, 41, and 42 are rejected under 35 U.S.C. 101 as not falling within

one of the four statutory categories of invention. While the claims recite a series of steps or acts

to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular

machine, or (2) transform underlying subject matter (such as an article or material) to a different

state or thing. See page 10 of *In Re Bilski* 88 USPQ2d 1385. The instant claims are neither

positively tied to a particular machine that accomplishes the claimed method steps nor transform

underlying subject matter, and therefore do not qualify as a statutory process. The key updating

method including steps of updating a key based on a user eviction is broad enough that the claim

could be completely performed mentally, verbally or without a machine nor is any

transformation apparent.

Claim Rejections - 35 USC § 102

12.   The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

13.   Claims 13-15, 19-21, 41-45 and 48-50 are rejected under 35 U.S.C. 102(b) based upon a

public use or sale of the invention. The Examiner holds that the invention of the instant

application was publicly used more than one year prior to the Applicant's filing for invention, as

can be seen by **Dynamic Cryptographic Context Management (DCCM): Report #1**

Architecture and System Design, which was first published on 02 June 1998. See MPEP §

2133.03(a).

14.   Claims 13-15, 19-21, 41-45 and 48-50 are rejected under 35 U.S.C. 102(b) as being

anticipated by **Dynamic Cryptographic Context Management (DCCM): Report #1**

Architecture and System Design, by David M. Balenson et al., hereinafter Balenson.

15.   As per claims 13 and 43, Balenson teaches apparatus and an environment that includes a

plurality of users, wherein a first user possesses a set of keys, said set of keys including a first

key that enables secure communication among a set of sets, said set of users including at least

said first user and a second user, a keying method, comprising:

        (a) upon eviction of at least said second user (pages 49, 115, 117), determining an

updated first key using information that includes said first key and a second key (page 10, i.e.

one-way function tree the keys are computed up, so in Figure 2 the keys for 1 and 2 are used to

compute the key for D), wherein said second key enables secure communication among a

subgroup of said set of users (page 1), wherein said subgroup does not include users subject to said eviction (Figure 4, pages 18, 20);

wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key (pages 34, 47, 54, 99, i.e. backward secrecy, forward secrecy, and prevent collusion, respectively);

wherein said updated first key is equal to F(first key, second key) (page 11, Figure 3, i.e. $k_i = f(k'_x, k'_y)$), wherein F() is a one-way function (page 10, Figure 2, i.e. one-way function tree). The Examiner has given very little patentable weight to the "wherein said determining…" it does not inform of any mechanics involved in the determining function; even if the Examiner has erred in his determination of whether the "wherein" clause should be afforded patentable weight, he has provided a showing of the properties as backward secrecy, forward secrecy, and collusion-resistance. See MPEP § 2111.04.

16.   With regards to claims 14, 15, 44, and 45, Balenson teaches wherein said updating occurs upon an eviction event, wherein only said second user or the second user and one or more other users are evicted (page 115, Figure 29).

17.   With regards to claim 41, Balenson teaches wherein said determining uses a one-way function (page 10, Figure 2, i.e. one-way function tree).

18.   Regarding claims 19 and 48, Balenson teaches wherein said determining uses only said first key and said second key (page 10, Figure 2, i.e. binary trees only account for two child nodes).

19.   Regarding claims 20, 21, 49, and 50, Balenson teaches wherein said subgroup includes only said first user or a plurality of users (Figure 4, pages 18, 20).

Conclusion

20.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

21.   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

22.   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf